IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	§	Group Art Unit: 2435
	§	
Emrys J. Williams	§	Examiner: Moran, Randal D.
	§	
	§	Atty. Dkt. No.: 5681-74900
	§	
	§	
	§	
Serial No.: 10/773,069	§	
	§	
	§	
Filed: February 5, 2004	§	
	§	
For: Method and System for	§	
Accepting a Pass Code	§	
	§	

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir/Madam:

Further to the Notice of Appeal filed May 19, 2009, Appellant presents this Appeal Brief. Appellant respectfully requests that the Board of Patent Appeals and Interferences consider this appeal.

I. REAL PARTY IN INTEREST

The subject application is owned by Sun Microsystems, Inc., a corporation organized and existing under and by virtue of the laws of the State of Delaware, and now having its principal place of business at 4150 Network Circle, Santa Clara, CA 95054.

II. RELATED APPEALS AND INTERFERENCES

No other appeals, interferences or judicial proceedings are known which would be related to, directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims 1-36, 38-52 and 54 are pending in the application and stand finally rejected. Claims 37 and 53 are cancelled. The rejection of claims 1-36, 38-52 and 54 is being appealed. A copy of claims 1-36, 38-52 and 54 is included in the Claims Appendix herein below.

IV. STATUS OF AMENDMENTS

No amendments have been submitted subsequent to the final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a method of accepting a pass code. (*See, e.g.,* p. 1, lines 6-7; p. 8, lines 11-12.) The method of accepting a pass code includes providing a user with a machine-generated challenge. (*See, e.g.,* p. 8, line 14; p. 21, lines 6-8; FIG. 6, challenge 620; p. 22, lines 10-14 and 16-17; and FIG. 8, steps 810 and 820.) The method of accepting a pass code also includes receiving, from a user-input device, user input capable of transforming the machine-generated challenge into a pass code allocated to the user, wherein the user input is dependent on the machine-generated challenge such that the user input capable of transforming the machine-generated challenge into the pass code is different for different machine-generated challenges. (*See, e.g.,* p. 8, lines 15-17 and 25-31; p. 14, lines 9-15; FIG. 3; p. 16, line 30 – p. 17, line 2; p. 18, lines 11-18; p. 21, lines 9-10; p. 22, lines 17-19.) The method of accepting a pass code also includes generating a response from the user input received from the user input device. (*See, e.g.,* p. 10, lines 6-8; p. 21, lines 13-16; p. 22, lines 17-19.) The method of accepting a pass code further includes transmitting the response to a remote authorisation unit to authenticate the response without transmitting the pass code to the remote authorisation unit and without generating the pass code from the user input prior to said transmitting, said response allowing the user to be validated at the authorisation unit compared to a predicted response based on knowledge of the challenge and a stored data record of the pass code. (*See, e.g.,* p. 10, lines 6-13; p. 21, lines 1-3 and 13-27; FIG. 6; p. 22, lines 17-19; FIG. 8, steps 830, 840 and 850; p. 22, line 30 – p. 23, line 4; p. 23, lines 9-12; p. 23, line 27 – p. 24, line 3.)

Independent claim 18 is directed to a terminal for use in accepting a pass code. (*See, e.g.,* p. 12, lines 31-32; FIG. 3.) The terminal includes an output for providing a user with a machine-generated challenge. (*See, e.g.* p. 21, lines 6-8; FIG. 6, challenge 620, display 301; p. 22, lines 10-14 and 16-17; and FIG. 8, steps 810 and 820.) The terminal also includes a user-input device for receiving user input capable of transforming the machine-generated challenge into a pass code allocated to the user, wherein the user input is dependent on the machine-generated challenge such that the

user input capable of transforming the machine-generated challenge into the pass code is different for different machine-generated challenges. (*See, e.g.,* p. 8, lines 15-17 and 25-31; p. 14, lines 9-15; FIG. 3; p. 16, line 30 – p. 17, line 2; p. 18, lines 11-18; p. 21, lines 9-10; p. 22, lines 17-19.) The terminal is configured to generate a response from the user input received from the user input device and transmit the response to a remote authorisation unit to authenticate the response, wherein the response is transmitted without the pass code and without the terminal generating the pass code from the response prior to transmitting, said response allowing the user to be validated at the authorisation unit compared to a predicted response based on knowledge of the challenge and a stored data record of the pass code. (*See, e.g.,* p. 10, lines 6-13; p. 21, lines 1-3 and 13-27; FIG. 6; p. 22, lines 17-19; FIG. 8, steps 830, 840 and 850; p. 22, line 30 – p. 23, line 4; p. 23, lines 9-12; p. 23, line 27 – p. 24, line 3.)

Independent claim 35 is directed to an apparatus. The apparatus includes means for providing a user with a machine-generated challenge. (*See, e.g.* p. 21, lines 6-8; FIG. 6, challenge 620, display 301; p. 22, lines 10-14 and 16-17; and FIG. 8, steps 810 and 820.) The apparatus also includes means for receiving user input capable of transforming the machine-generated challenge into a pass code allocated to the user, wherein the user input is dependent on the machine-generated challenge such that the user input capable of transforming the machine-generated challenge into the pass code is different for different machine-generated challenges. (*See, e.g.,* p. 8, lines 15-17 and 25-31; p. 14, lines 9-15; FIG. 3; p. 16, line 30 – p. 17, line 2; p. 18, lines 11-18; p. 21, lines 9-10; p. 22, lines 17-19.) The apparatus also includes means for generating a response from the user input received from the user input device. (*See, e.g.,* p. 21, lines 13-16; p. 22, lines 17-19.) The apparatus further includes means for transmitting the response to a remote authorisation unit to authenticate the response without transmitting the pass code to the remote authorisation unit and without generating the pass code from the user input prior to said transmitting. (*See, e.g.,* p. 21, lines 1-3 and 13-27; FIG. 6; p. 22, lines 17-19; FIG. 8, steps 830, 840 and 850; p. 22, line 30 – p. 23, line 4; p. 23, lines 9-12; p. 23, line 27 – p. 24, line 3.)

Independent claim 36 is directed to a method for using a pass code to validate a user. (*See, e.g.* p. 1, lines 6-7; p. 10, lines 31-32.) The method for using a pass code to validate a user includes receiving a request from a user for validation. (*See, e.g.* p. 10, line 32 – p. 11, line 1.) The method for using a pass code to validate a user also includes generating a challenge in response to said request and providing the user with the challenge. (*See, e.g.* p. 8, line 14; p. 11, lines 1-2; p. 21, lines 6-7; FIG. 6, challenge 620; p. 22, lines 10-14 and 16-17; and FIG. 8, steps 810 and 820.) The method for using a pass code to validate a user also includes receiving, from a user-input device, user input capable of transforming the challenge into a pass code allocated to the user, wherein the user input is dependent on the challenge such that the user input capable of transforming the challenge into the pass code is different for different challenges. (*See, e.g.,* p. 8, lines 15-17 and 25-31; p. 11, lines 2-3; p. 14, lines 9-15; FIG. 3; p. 16, line 30 – p. 17, line 2; p. 18, lines 11-18; p. 21, lines 9-10; p. 22, lines 17-19.) The method for using a pass code to validate a user also includes generating a response from the user input received from the user input device, wherein the response is not the pass code. (*See, e.g.,*; p. 21, lines 1-3 and 13-16; p. 22, lines 17-19; p. 22, line 30 – p. 23, line 4; p 23, lines 9-12.) The method for using a pass code to validate a user also includes generating a predicted response based on knowledge of the challenge and a stored version of the pass code. (*See, e.g.* p. 10, lines 6-13; FIG. 8, steps 840 and 850.) The method for using a pass code to validate a user further includes validating the user on the basis of said response compared to the predicted response, wherein neither the response nor the predicted response is the pass code. (*See, e.g.* p. 10, lines 11-13; p. 11, lines 3-4.)

Independent claim 38 is directed to a computer program product comprising instructions encoded on a storage medium. (*See, e.g.* p. 11, lines 15-25.) The instructions, when loaded into a machine, cause the machine to provide a user with a machine-generated challenge. (*See, e.g.,* p. 8, line 14; p. 16, line 30 – p. 17, line 2; p. 21, lines 6-8; FIG. 6, challenge 620; p. 22, lines 10-14 and 16-17; and FIG. 8, steps 810 and 820.) The instructions also cause the machine to receive, from a user-input device, user input capable of transforming the machine-generated challenge into a pass code allocated to the user, wherein the user input is dependent on the machine-generated challenge such

that the user input capable of transforming the machine-generated challenge into the pass code is different for different machine-generated challenges. (*See, e.g.,* p. 8, lines 15-17 and 25-31; p. 14, lines 9-15; FIG. 3; p. 18, lines 11-18; p. 21, lines 9-10; p. 22, lines 17-19.) The instructions also cause the machine to generate a response to the challenge from the user input received from the user input device. (*See, e.g.,* p. 10, lines 6-8; p. 21, lines 13-16; p. 22, lines 17-19.) The instructions also cause the machine to transmit the response to a remote authorisation unit to authenticate the response, without transmitting the pass code to the remote authorization unit and without generating the pass code from the response prior to said transmitting, said response allowing the user to be validated at the authorisation unit compared to a predicted response based on knowledge of the challenge and a stored data record of the pass code. (*See, e.g.,* p. 10, lines 6-13; p. 21, lines 1-3 and 13-27; FIG. 6; p. 22, lines 17-19; FIG. 8, steps 830, 840 and 850; p. 22, line 30 – p. 23, line 4; p. 23, lines 9-12; p. 23, line 27 – p. 24, line 3.)

The summary above describes various examples and embodiments of the claimed subject matter; however, the claims are not necessarily limited to any of these examples and embodiments. The claims should be interpreted based on the wording of the respective claims.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-16, 18-33 and 35-53 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over Hoover (U.S. Patent 6,209,102), (hereinafter "Hoover").

2. Claims 17, 34 and 54 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over Hoover in view of Funk (U.S. Patent 5,721,779), (hereinafter "Funk").

VII. ARGUMENT

First ground of rejection:

The Examiner rejected claims 1-16, 18-33 and 35-53 under 35 U.S.C. § 103(a) as being unpatentable over Hoover. Appellant traverses the rejection of these claims for at least the following reasons. Different groups of claims are addressed under their respective subheadings.

Claims 1-16, 18-33 and 38-52:

1. The cited art clearly fails to teach or suggest *transmitting the response to a remote authorisation unit to authenticate the response without transmitting the pass code to the remote authorisation unit and without generating the pass code from the user input prior to said transmitting.*

Hoover is directed to protecting a user's access code from an attacker while the user is inputting the access code into a computing environment. Specifically, Hoover's goal is to protect the user against an attacker that has access to the computing environment, "either through software or by physically looking over the user's shoulder." (Hoover, col. 2, lines 65-68). The attacker software described by Hoover "collects, and saves to a file, all the keystrokes that the user types on his keyboard" (Hoover, col. 1, lines 25-26) and/or captures "the locations ... of mouse clicks and [uses] them to deduce the characters indicated." (Hoover, col. 1, lines 36-38). Hoover describes a system for protecting user input of an access code (e.g., PIN numbers or passwords) by displaying pseudo-randomized characters and allowing the user to change (e.g., increment and decrement) the characters until the access code is displayed. Hoover does not protect the access code during transmission, but rather Hoover protects the access code at the time of user input. Hoover does not teach or suggest transmitting a response to a remote authorisation unit to authenticate the response **without transmitting the pass code to the**

remote authorisation unit and without **generating the pass code prior to said transmitting**, as recited in Appellant's claim 1.

On p. 3 of the Final Action dated February 19, 2009, the Examiner admits, "Hoover does not explicitly disclose transmitting the response to a remote authorization unit to authenticate the response without transmitting the pass code to the remote authorization unit and without generating the pass code from the response prior to said transmitting." The Examiner cites col. 2, lines 56-61 of Hoover and asserts, "it would have been obvious to one of ordinary skill in the art at the time of the invention to transmit the offset digital sequence without transmitting the actual pass code for the benefit of protecting a user's PIN, password, or other access code..." However, the passage of Hoover cited by the Examiner discloses a row of digits containing "an initially random PIN digit sequence" (Hoover, col. 2, line 57), an "offset digit sequence row" (Hoover, col. 2, line 60) that creates the correct PIN sequence when added to the random PIN digit sequence, **and** a "**resulting correct PIN digit sequence** [that] could be displayed adjacent to the other two rows." (Hoover, col. 2, lines 61-63). (emphasis added). The Examiner's unfounded speculation is counter to the explicit teachings of Hoover. As shown above, Hoover states that the action of adding the initial random digit sequence to the user inputted offset digit sequence produces the actual PIN that is stored and available for transmission. Hoover clearly teaches that the actual PIN is generated. Furthermore, transmission of only the offset digital sequence and not the actual PIN would require that the recipient of the offset digital sequence also have knowledge of the initial random sequence in order to create the actual PIN for validation. However, the recipient is not described as having this information in Hoover's system. Thus, Hoover's system could not even function if the offset sequence was sent instead of the actual PIN.

Furthermore, Hoover explicitly discloses transmitting the actual PIN:

> In an Internet environment, the user-selectable fields could be implemented (i) using Javascript on a web page to send the PIN to a common gateway interface (CGI) script or active server page, (ii) using a Java applet on a web page to send the PIN to a CGI script or active server page, (iii) using a plug-in with a GUI on a web page to send the PIN to a CGI script or active server page, (iv) using a specialized network application with a GUI to send results by a network

connection to a server application, or (v) using a specialized network application with command line input. (Hoover, col. 3, lines 30-40). (emphasis added)

In this passage, Hoover clearly discloses that a PIN is sent to a gateway or an active server page. Thus, Hoover clearly generates and transmits an actual PIN, or access code. In contrast, Appellant's claim requires transmitting the response (i.e., the transformation of the challenge) received from the user input device to a remote authorization unit without including the pass code and without the pass code having even been generated.

In the Response to Arguments section on p. 8 of the Final Action dated February 19, 2009, in remarks directed to claim 1, the Examiner asserts that Hoover, in col. 2, lines 44-53 discloses "a user being presented a random 6-digit number which must be transformed into the passcode. The passcode is never entered by the user, the user simply increments the digits by a +1 or -1 but never actually enters the passcode." Appellant notes that this passage of Hoover, on lines 49-52, states, "To select his PIN, the user cursors through the digits. At each digit, he hits the up or down arrow key (to increment the digit by +1 or -1) an appropriate number of times **until the desired digit appears**." (emphasis added) After the user's entry of incrementing each digit, **the actual PIN** is displayed on the screen. Thus, this passage clearly discloses generating an actual access code and is contrary to the Examiner's assertion that Hoover teaches not generating the passcode prior to said transmitting. Hoover explicitly states that the actual PIN is generated by the system prior to transmitting a response to a remote authorization unit. In contrast, Appellant's claim requires that the passcode is not generated prior to transmission.

Hoover further discloses generating the actual PIN in col. 2, lines 40-43: "The current PIN could be displayable adjacent to the bingo card (FIG. 1) or the selected PIN characters could be highlighted on the bingo card, e.g. by changing the color or shading of the selected characters." Hoover also further discloses sending an actual access code in col. 3, lines 16-19: "Based on the display, the user provides feedback (in the form of an entered access code) via input device 340, which is passed back through processor 320

to access control program 350." Thus, Hoover clearly and explicitly teaches sending the actual access code (i.e., password) to local processor 320 for validation.

As shown above, Hoover clearly discloses generating an actual access code and sending the actual access code for validation. Accordingly, Appellant asserts that Hoover cannot be said to teach or suggest transmitting the response to a remote authorisation unit to authenticate the response **without transmitting the pass code to the remote authorisation unit** and **without generating the pass code from the user input** prior to said transmitting. Hoover's stated purpose is to protect an access code at the time of user input. Hoover does not pertain to protecting an access code during transmission, and furthermore, does not disclose a recipient of a user response capable of interpreting a user response that is not a complete access code. Therefore, a *prima facie* rejection has not been established.

2. The cited art clearly fails to teach or suggest *transmitting the response to a remote authorisation unit ... said response allowing the user to be validated at the authorisation unit compared to a predicted response based on knowledge of the challenge and a stored data record of the pass code.*

The Examiner **fails to provide any remarks** directed to a remote authorization unit using a predicted response based on knowledge of a challenge and a stored data record of a pass code to validate a user. Thus, a *prima facie* rejection has not been stated. Hoover only discloses validating a user based on an actual access code. Hoover describes, "granting, to said user, access to a service if said accepted plurality of selections correctly correspond to said access code" (Hoover, col. 4, lines 34-36). Hoover does not teach or suggest any type of predicted response based on knowledge of a challenge and a stored data record of a pass code. Nor does Hoover teach or suggest validating a user based on this predicted response. Furthermore, as shown above, Hoover's system sends only the actual access code to be used for granting access to a user. Thus, Hoover's system is incapable of validating a user by comparing a user response (that is not the actual pass code) to a predicted response based on knowledge of

a challenge and a stored data record of a pass code. Accordingly, Appellant asserts that Hoover does not teach or suggest transmitting the response to a remote authorisation unit … said response allowing the user to be validated at the authorisation unit compared to a predicted response based on knowledge of the challenge and a stored data record of the pass code.

For at least the reasons stated above, Appellant asserts that the Examiner has failed to establish a *prima facie* rejection. The rejection of claim 1 is unsupported by the evidence of record and reversal thereof is respectfully requested.

Independent claims 18 and 38 include the limitations *transmitting the response to a remote authorisation unit to authenticate the response without transmitting the pass code to the remote authorisation unit and without generating the pass code from the user input prior to said transmitting* and *said response allowing the user to be validated at the authorisation unit compared to a predicted response based on knowledge of the challenge and a stored data record of the pass code* or similar limitations. Therefore, the arguments presented above regarding these limitations apply with equal force to these claims as well. Thus, the Examiner has not established a *prima facie* rejection in regard to these claims.

Claim 35:

1. The cited art clearly fails to teach or suggest *means for transmitting the response to a remote authorisation unit to authenticate the response without transmitting the pass code to the remote authorisation unit and without generating the pass code from the user input prior to said transmitting.*

Hoover is directed to protecting a user's access code from an attacker while the user is inputting the access code into a computing environment. Specifically, Hoover's goal is to protect the user against an attacker that has access to the computing environment, "either through software or by physically looking over the user's shoulder."

(Hoover, col. 2, lines 65-68). The attacker software described by Hoover "collects, and saves to a file, all the keystrokes that the user types on his keyboard" (Hoover, col. 1, lines 25-26) and/or captures "the locations … of mouse clicks and [uses] them to deduce the characters indicated." (Hoover, col. 1, lines 36-38). Hoover describes a system for protecting user input of an access code (e.g., PIN numbers or passwords) by displaying pseudo-randomized characters and allowing the user to change (e.g., increment and decrement) the characters until the access code is displayed. Hoover does not protect the access code during transmission, but rather Hoover protects the access code at the time of user input. Hoover does not teach or suggest transmitting a response to a remote authorisation unit to authenticate the response **without transmitting the pass code to the remote authorisation unit** and without **generating the pass code prior to said transmitting**, as recited in Appellant's claim 35.

On p. 3 of the Final Action dated February 19, 2009, the Examiner admits, "Hoover does not explicitly disclose transmitting the response to a remote authorization unit to authenticate the response without transmitting the pass code to the remote authorization unit and without generating the pass code from the response prior to said transmitting." The Examiner cites col. 2, lines 56-61 of Hoover and asserts, "it would have been obvious to one of ordinary skill in the art at the time of the invention to transmit the offset digital sequence without transmitting the actual pass code for the benefit of protecting a user's PIN, password, or other access code…" The passage of Hoover cited by the Examiner discloses a row of digits containing "an initially random PIN digit sequence" (Hoover, col. 2, line 57), an "offset digit sequence row" (Hoover, col. 2, line 60) that creates the correct PIN sequence when added to the random PIN digit sequence, **and** a "**resulting correct PIN digit sequence** [that] could be displayed adjacent to the other two rows." (Hoover, col. 2, lines 61-63). (emphasis added). The Examiner's unfounded speculation is counter to the explicit teachings of Hoover. As shown above, Hoover states that the action of adding the initial random digit sequence to the user inputted offset digit sequence produces the actual PIN that is stored and available for transmission. Hoover clearly teaches that the actual PIN is generated. Therefore, it would not be obvious to transmit the offset digital sequence because the actual PIN is

clearly available for transmission. Furthermore, transmission of only the offset digital sequence and not the actual PIN would require that the recipient of the offset digital sequence also have knowledge of the initial random sequence in order to create the actual PIN for validation. This is not the case in Hoover's system. Hoover clearly does not teach or suggest sending the initial random sequence or a recipient having knowledge of the initial random sequence.

Furthermore, Hoover explicitly discloses sending the PIN in an Internet environment:

> In an Internet environment, the user-selectable fields could be implemented (i) using Javascript on a web page **to send the PIN to a common gateway interface (CGI) script or active server page**, (ii) using a Java applet on a web page **to send the PIN to a CGI script or active server page**, (iii) using a plug-in with a GUI on a web page to send the PIN to a CGI script or active server page, (iv) using a specialized network application with a GUI to send results by a network connection to a server application, or (v) using a specialized network application with command line input. (Hoover, col. 3, lines 30-40). (emphasis added)

In this passage, Hoover clearly discloses that a PIN is sent to a gateway or an active server page. Thus, Hoover clearly generates and transmits an actual PIN, or access code. In contrast, Appellant's claim requires transmitting the response (i.e., the transformation of the challenge) received from the user input device to a remote authorization unit without including the pass code and without the pass code having even been generated.

In the Response to Arguments section on p. 8 of the Final Action dated February 19, 2009, in remarks directed to claim 1, the Examiner asserts that Hoover, in col. 2, lines 44-53 discloses "a user being presented a random 6-digit number which must be transformed into the passcode. The passcode is never entered by the user, the user simply increments the digits by a +1 or -1 but never actually enters the passcode." Appellant notes that this passage of Hoover, on lines 49-52, states, "To select his PIN, the user cursors through the digits. At each digit, he hits the up or down arrow key (to increment the digit by +1 or -1) an appropriate number of times **until the desired digit appears**." (emphasis added) After the user's entry of incrementing each digit, **the actual PIN** is displayed on the screen. Thus, this passage clearly discloses generating an actual access

code and is contrary to the Examiner's assertion that Hoover teaches without generating the passcode from the user prior to said transmitting. The user input described in this passage may not be digits corresponding to the actual PIN; however, the user input does result in the actual PIN being generated by the system. Appellant's claim requires that the passcode is not generated prior to transmission of the user response.

Hoover further discloses generating the actual PIN in col. 2, lines 40-43: "The current PIN could be displayable adjacent to the bingo card (FIG. 1) or the selected PIN characters could be highlighted on the bingo card, e.g. by changing the color or shading of the selected characters." Hoover also further discloses sending an actual access code in col. 3, lines 16-19: "Based on the display, the user provides feedback (in the form of an entered access code) via input device 340, which is passed back through processor 320 to access control program 350." Hoover clearly discloses sending the actual access code (i.e., password) to local processor 320 for validation.

As shown above, Hoover clearly discloses generating an actual access code and sending the actual access code for validation. Accordingly, Appellant asserts that Hoover cannot be said to teach or suggest transmitting the response to a remote authorisation unit to authenticate the response **without transmitting the pass code to the remote authorisation unit** and **without generating the pass code from the user input** prior to said transmitting.

For at least the reasons stated above, Appellant asserts that the Examiner has failed to establish a *prima facie* rejection. The rejection of claim 35 is unsupported by the evidence of record and reversal thereof is respectfully requested.

Claim 36:

1. The cited art clearly fails to teach or suggest *generating a predicted response based on knowledge of the challenge and a stored version of the pass code.*

The Examiner **fails to provide any remarks** directed to generating a predicted response based on knowledge of a challenge and a stored version of a pass code. Thus, a *prima facie* rejection has not been stated. Hoover discloses nothing regarding generating a predicted response of any sort, much less a predicted response based on knowledge of a challenge and a stored version of a pass code. Hoover, in col. 2, lines 57-63, clearly discloses that an actual access code is generated. Furthermore, Hoover, in col. 3, lines 30-40, clearly discloses that the actual access code is sent. Hoover does not disclose sending or comparing any type of user response other than the actual access code. Furthermore, Hoover does not protect the access code during transmission, but rather Hoover protects the access code at the time of user input. Therefore, Hoover has no motivation to generate a prediction of a user response based on knowledge of a challenge presented to the user and a stored version of a pass code.

2. The cited art clearly fails to teach or suggest *validating the user on the basis of said response compared to the predicted response, wherein neither the response nor the predicted response is the pass code.*

The Examiner **fails to provide any remarks** directed to validating the user on the basis of a user response compared to a predicted response, wherein neither the user response nor the predicted response is the pass code. Thus, a *prima facie* rejection has not been stated. Hoover only discloses validating a user based on an actual access code. Hoover describes, "granting, to said user, access to a service if said accepted plurality of selections correctly correspond to said access code" (Hoover, col. 4, lines 34-36). Thus, Hoover clearly compares a user's input (i.e. selections) against an expected access code in order to determine whether access should be granted. Hoover does not teach or suggest any type of predicted response based on knowledge of a challenge and a stored data record of a pass code. Nor does Hoover teach or suggest validating a user based on this predicted response. Furthermore, as shown above, Hoover's system sends only an actual access code to be used for granting access to a user. Thus, Hoover's system is incapable of validating a user by comparing a user response that is not a pass code to a predicted response based on knowledge of a challenge and a stored data record of a pass

code. Accordingly, Appellant asserts that Hoover does not teach or suggest validating the user on the basis of said response compared to the predicted response, wherein neither the response nor the predicted response is the pass code.

For at least the reasons stated above, Appellant asserts that the Examiner has failed to establish a *prima facie* rejection. The rejection of claim 36 is unsupported by the evidence of record and reversal thereof is respectfully requested.

Second ground of rejection:

The Examiner rejected claims 17, 34 and 54 under 35 U.S.C. § 103(a) as being unpatentable over Hoover in view of Funk. Appellant traverses the rejection of these claims for at least the following reasons. Different groups of claims are addressed under their respective subheadings.

Claims 17, 34 and 54:

1. The cited art clearly fails to teach or suggest *using the response to encrypt said communications challenge and transmitting the encrypted communications challenge to the authorisation unit; thereby allowing the response to be validated by said authorisation unit using said stored data record of the pass code.*

On p. 7 of the Final Action dated February 19, 2009, the Examiner admits Hoover fails to teach using the response to encrypt the communications challenge and relies on Funk, citing column 4, lines 50-52. Funk is directed towards utilizing a challenge and response handshake to allow a server to authenticate a client based on a password. Column 4, lines 50-53 of Funk state: "The client can generate this response signal by employing the same one-way commutative function to encrypt the challenge signal, C, with one valid password." Funk uses the actual password to generate the response. Column 4, line 59 of Funk provides the following formula: Response=$F(C,$ Password)=$C^{password}$ mod q. In contrast, Appellant's claim requires using the user

response (i.e., transformation of the challenge), not the actual pass code, to encrypt the communications challenge. Both Hoover and Funk use the actual PIN or password in their respective designs. Thus, Funk combined with Hoover would not result in Appellant's claimed invention.

In the Response to Arguments section on p. 8 of the Final Action dated February 19, 2009, the Examiner submits, "Funk is used to show encryption and is not used to show the transmission of the response." The Examiner appears to have missed the point of Appellant's argument. Both Hoover and Funk use the actual PIN or password in their respective designs. Neither reference, whether considered alone or in combination, teaches or suggests using the response (that is not the PIN/password) to encrypt the communications challenge and transmit the encrypted communications challenge to the authorisation unit.

For at least the reasons stated above, Appellant asserts that the Examiner has failed to establish a *prima facie* rejection. The rejection of claim 17 is unsupported by the evidence of record and reversal thereof is respectfully requested.

Claims 34 and 54 recite limitations similar to those discussed above, and were rejected for the same reasons as claim 17. Therefore, the arguments presented above apply with equal force to this claim, as well. Thus, the Examiner has not established a *prima facie* rejection in regard to these claims.

CONCLUSION

For the foregoing reasons, it is submitted that the Examiner's rejection of claims 1-36, 38-52 and 54 was erroneous, and reversal of the Examiner's decision is respectfully requested.

The Commissioner is authorized to charge any fees that may be due to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5681-74900/RCK. This Appeal Brief is submitted with a return receipt postcard.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Appellant

Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
(512) 853-8850

Date: July 20, 2009

VIII. CLAIMS APPENDIX

The claims on appeal are as follows.

1. A method of accepting a pass code, comprising:

providing a user with a machine-generated challenge; and

receiving, from a user-input device, user input capable of transforming the machine-generated challenge into a pass code allocated to the user, wherein the user input is dependent on the machine-generated challenge such that the user input capable of transforming the machine-generated challenge into the pass code is different for different machine-generated challenges;

generating a response from the user input received from the user input device; and

transmitting the response to a remote authorisation unit to authenticate the response without transmitting the pass code to the remote authorisation unit and without generating the pass code from the user input prior to said transmitting, said response allowing the user to be validated at the authorisation unit compared to a predicted response based on knowledge of the challenge and a stored data record of the pass code.

2. The method of claim 1, wherein said challenge is independent of said pass code.

3. The method of claim 1, further comprising generating a new challenge for each user validation.

4. The method of claim 3, wherein said challenge is generated on a random basis.

5. The method of claim 3, wherein the challenge is generated in response to receiving a request from a user for validation.

6. The method of claim 1, wherein providing a user with a challenge comprises displaying the challenge to the user.

7. The method of claim 6, wherein the challenge is displayed to the user in such a manner as to prevent third parties from viewing the challenge.

8. The method of claim 1, wherein the user input from the user-input device is received as a set of one or more modifications to be applied to the challenge so that it matches the pass code allocated to the user.

9. The method of claim 8, wherein said set of one or more modifications is received as directional input from the user.

10. The method of claim 9, wherein said directional input is received as the result of the user pressing one or more arrow keys that increment or decrement the challenge by a fixed amount.

11. The method of claim 1, wherein said challenge has the same number of characters as the pass code allocated to the user.

12. The method of claim 11, wherein said transformation is specified individually for each character of the challenge.

13. The method of claim 12, further comprising receiving an indication from the user that the transformation for a different character is about to be entered.

14. The method of claim 1, further comprising receiving an indication from the user that the user input to transform the challenge has been completely entered.

15. The method of claim 1, further comprising generating a pass code from the challenge and from the response.

16. The method of claim 15, wherein the response is validated by comparing the generated pass code with the stored data record of the pass code.

17. The method of claim 1, further comprising:

receiving a communications challenge from the remote authorisation unit that has access to said stored data record of the pass code;

using the response to encrypt said communications challenge; and

transmitting the encrypted communications challenge to the remote authorisation unit;

thereby allowing the response to be validated by said remote authorisation unit using said stored data record of, the pass code.

18. A terminal for use in accepting a pass code, comprising:

an output for providing a user with a machine-generated challenge; and

a user-input device for receiving user input capable of transforming the machine-generated challenge into a pass code allocated to the user, wherein the user input is dependent on the machine-generated challenge such that the user

input capable of transforming the machine-generated challenge into the pass code is different for different machine-generated challenges;

wherein said terminal is further configured to generate a response from the user input received from the user input device and transmit the response to a remote authorisation unit to authenticate the response, wherein the response is transmitted without the pass code and without the terminal generating the pass code from the response prior to transmitting, said response allowing the user to be validated at the authorisation unit compared to a predicted response based on knowledge of the challenge and a stored data record of the pass code.

19. The terminal of claim 18, wherein said challenge is independent of said pass code.

20. The terminal of claim 18, wherein a new challenge is generated for each user validation.

21. The terminal of claim 20, wherein said challenge is generated on a random basis.

22. The terminal of claim 20, wherein the challenge is generated in response to receiving a request from a user for validation.

23. The terminal of claim 18, further comprising a display, wherein the challenge is provided to the user on the display.

24. The terminal of claim 23, wherein the terminal is configured to prevent parties other than the user from viewing the challenge on the display.

25. The terminal of claim 18, wherein the user input from the user-input device is received as a set of one or more modifications to be applied to the challenge so that it matches the pass code allocated to the user.

26. The terminal of claim 25, wherein said set of one or more modifications is received as directional input from the user.

27. The terminal of claim 26, wherein the user-input device comprises one or more arrow keys that increment or decrement the challenge by a fixed amount.

28. The terminal of claim 18, wherein said challenge has the same number of characters as the pass code allocated to the user.

29. The terminal of claim 28, wherein said transformation is specified individually for each character of the challenge.

30. The terminal of claim 29, wherein the user-input device comprises a key for receiving an indication from the user that the transformation for a different character is about to be entered.

31. The terminal of claim 18, wherein the user-input device comprises a key for receiving an indication from the user that the user input to transform the challenge has been completely entered.

32. The terminal of claim 18, wherein the pass code is generated from the challenge and from the user input from the user-input device.

33. The terminal of claim 32, wherein the user is validated by comparing the generated pass code with a stored data record of the pass code.

34. The terminal of claim 18, further comprising a communications link with the remote authorisation unit that has access to a stored data record of the pass code, wherein the terminal receives a communications challenge from said remote authorisation unit and uses a response generated from the user input to encrypt said communications challenge, and wherein the encrypted communications challenge is transmitted to the remote authorisation unit, thereby allowing the response to be validated by said remote authorisation unit against said stored data record of the pass code.

35. An apparatus, comprising:

means for providing a user with a machine-generated challenge;

means for receiving user input capable of transforming the machine-generated challenge into a pass code allocated to the user, wherein the user input is dependent on the machine-generated challenge such that the user input capable of transforming the machine-generated challenge into the pass code is different for different machine-generated challenges;

means for generating a response from the user input received from the user input device, and;

means for transmitting the response to a remote authorisation unit to authenticate the response without transmitting the pass code to the remote authorisation unit and without generating the pass code from the user input prior to said transmitting.

36. A method for using a pass code to validate a user, comprising:

receiving a request from a user for validation;

generating a challenge in response to said request;

providing the user with the challenge;

receiving, from a user-input device, user input capable of transforming the challenge into a pass code allocated to the user, wherein the user input is dependent on the challenge such that the user input capable of transforming the challenge into the pass code is different for different challenges;

generating a response from the user input received from the user input device, wherein the response is not the pass code;

generating a predicted response based on knowledge of the challenge and a stored version of the pass code; and

validating the user on the basis of said response compared to the predicted response, wherein neither the response nor the predicted response is the pass code.

38. A computer program product comprising instructions encoded on a storage medium, said instructions when loaded into a machine causing the machine:

to provide a user with a machine-generated challenge; and

receive, from a user-input device, user input capable of transforming the machine-generated challenge into a pass code allocated to the user, wherein the user input is dependent on the machine-generated challenge such that the user input capable of transforming the machine-generated challenge into the pass code is different for different machine-generated challenges;

generate a response to the challenge from the user input received from the user input device; and

transmitting the response to a remote authorisation unit to authenticate the response, without transmitting the pass code to the remote authorization unit and without generating the pass code from the response prior to said transmitting, said response allowing the user to be validated at the authorisation unit compared to a predicted response based on knowledge of the challenge and a stored data record of the pass code.

39. The computer program product of claim 38, wherein said challenge is independent of said pass code.

40. The computer program product of claim 38, wherein said instructions further cause the machine to generate a new challenge for each user validation.

41. The computer program product of claim 40, wherein the challenge is generated in response to receiving a request from a user for validation.

42. The of computer program product of claim 40, wherein said challenge is generated on a random basis.

43. The computer program product of claim 38, wherein providing a user with a challenge comprises displaying the challenge to the user.

44. The computer program product of claim 43, wherein the challenge is displayed to the user in such a manner as to prevent third parties from viewing the challenge.

45. The computer program product of claim 38, wherein the user input from the user-input device is received as a set of one or more modifications to be applied to the challenge so that it matches the pass code allocated to the user.

46. The computer program product of claim 45, wherein said set of one or more modifications is received as directional input from the user.

47. The computer program product of claim 46, wherein said directional input is received as the result of the user pressing one or more arrow keys that increment or decrement the challenge by a fixed amount.

48. The computer program product of claim 38, wherein said challenge has the same number of characters as the pass code allocated to the user.

49. The computer program product of claim 48, wherein said transformation is specified individually for each character of the challenge.

50. The computer program product of claim 49, wherein said instructions further cause the machine to receive an indication from the user-input device that the transformation for a different character is about to be entered.

51. The computer program product of claim 38, wherein said instructions further cause the machine to receive an indication from the user that the user input to transform the challenge has been completely entered.

52. The computer program product of claim 38, wherein said instructions further cause the machine to generate the pass code from the challenge and from the user input from the user-input device.

54. The computer program product of claim 38, wherein the instructions further cause the machine:

to receive a communications challenge from the remote authorisation unit that has access to a stored data record of the pass code;

to use the a response generated from the user input to encrypt said communications challenge; and

to transmit the encrypted communications challenge to the remote authorisation unit, thereby allowing the response to be validated by said remote authorisation unit using said stored data record of the pass code.

IX. EVIDENCE APPENDIX

No evidence submitted under 37 CFR §§ 1.130, 1.131 or 1.132 or otherwise entered by the Examiner is relied upon in this appeal.

X. RELATED PROCEEDINGS APPENDIX

There are no related proceedings.